Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward

Marthie Grobler, Joey Jansen van Vuuren, and Louise Leenen

Council for Scientific and Industrial Research, Pretoria, South Africa
{mgrobler1,jjvvuuren,lleenen}@csir.co.za

Abstract. Cyber security is an important aspect of National Security and the safekeeping of a Nation's constituency and resources. In South Africa, the focus on cyber security is especially prominent since many geographical regions are incorporated into the global village in an attempt to bridge the digital divide. This article reflects on current research done in South Africa with regard to a cyber security policy, and proposes the development of methodologies and frameworks that will enable the implementation of such a policy. The focus of this article is the use of an ontology-based methodology to identify and propose a formal, encoded description of the cyber security strategic environment. The aim of the ontology is to identify and represent the multi-layered organisation of players and their associated roles and responsibilities within the cyber security environment. This will contribute largely to the development, implementation and rollout of a national cyber security policy in South Africa.

Keywords: cyber security, ontology, policy, security awareness.

1 Introduction

Information and its related infrastructures are fundamental to cyber security and the implementation of an associated cyber security policy. On the one hand, cyber security pertains to the maintenance of National Security and the interests of citizens; whilst, on the other hand, it can refer to politically motivated hacking to conduct sabotage and espionage against specific nation states. Therefore, the rationale behind national cyber security is to enable the safekeeping of a Nation's constituency and its associated organisational, human, financial, technological and informational resources. This is done to facilitate the achievement of its National objectives [9].

In South Africa, cyber security has been identified as a critical component contributing towards National Security. More geographical regions of South Africa are becoming integrated into the global village, necessitating additional government initiatives aimed at bridging the digital divide and addressing cyber security. One of these initiatives is the development and implementation of a South African specific cyber security policy.

Despite the African continent's recent explosive growth in information and communication technologies, Africa is generally considered as being spared the global high levels of cyber crimes. Although this is often attributed to its traditionally low

M.D. Hercheui et al. (Eds.): HCC10 2012, IFIP AICT 386, pp. 215–225, 2012.

Internet penetration levels with only 139 million Internet users out of a population of more than 2 billion people [16], Africans tend to increasingly fall prey to online predators [14]. In addition, many of the factors that traditionally make African countries more vulnerable (such as increasing bandwidth, use of wireless technologies and infrastructure, high levels of computer illiteracy, ineffective or insufficient legislation to deal with cyber attacks and threats) further expose these countries' crucial infrastructures to cyber risks [12]; hence an effective cyber security policy is urgently needed in order to be able to respond to these risks. A national cyber security policy framework would *"bolster and improve South Africa's cyber security"* [14].

This article will look at the current and future research and development done towards the implementation of a cyber security policy in South Africa. It will present retrospective reflections, as well as proposed future work on selected methodologies and frameworks that will enable the implementation of such a policy. The innovative contribution of this research lies in the argument that an ontology can assist in defining a model that describes the relationships between different cyber security components. Section 2 summarises the development process of a cyber security policy for South Africa. Section 3 gives an overview of cyber security research in South Africa and discusses ways in which the research relates to the development of a cyber security policy. From these two sections it becomes clear that a descriptive model of the cyber security environment in South Africa is required. This leads to a proposal for the development of a cyber security ontology in Section 4. Future research is discussed in Section 5 and the article is concluded in Section 6.

2 Background

South Africa has a huge responsibility to promote cyber security awareness, since the State can be held responsible for wrongful acts committed inside a country, and is obliged to fulfil the interests of the entire international community. As a result, the national cyber security policy framework for South Africa is a long time coming, and initial workshops on the topic were held already in January 2009. Despite the time and effort put into the development of the policy framework, the process of implementation is still not complete.

At the time of writing, the initial published draft version of the policy declared milestones for the imminent establishment of the security CSIRT (Computer Security Incident Response team) and the sector CSERT (Computer Security Emergency Response team) [8]. The decision was made in February 2012 that the Department of State Security should take over responsibility from the Department of Communications (DOC) for drawing the government's policy on cyber crime. In 2010, a similar decision was made to reassign the mandate from the Department of Science and Technology (DST) to the DOC [10].

Given the current status of the policy framework in South Africa, it is agreed that there is not enough emphasis on the national cyber security policy, although reference is made to the policy as the overarching strategy that must guide cyber security. In

response, this article proposes five elements as a foundation for the South African cyber security policy requirements: (i) political will; (ii) adapted organisational structures; (iii) identifying accurate proactive and reactive measures; (iv) reducing criminal opportunities; and (iv) education and awareness [9].

It is recommended that these five elements should be present in developing a national strategy for an effective cyber security approach and culture. The next section addresses these elements in more detail, with a preliminary mapping of current South African cyber security research to determine the current state and progress of a cyber security policy implementation. These elements fit with the South African proposed multi-faceted approach to reduce cyber crime [7].

3 Current State of Cyber Security Research in South Africa

The dynamic and volatile nature of the Internet and the cyber domain in general make cyber security research within South Africa an important area to address. Since the cyber domain is inherently globalised, it cannot truly be considered in isolation or on a purely national basis [18]. As such, the South African Justice minister, Jeff Radebe, stated at a parliamentary briefing in February 2012 that finalising specific cyber crime plans would be a priority in 2012 [7]. In addition, the DOC stated that its *"decision to boost cyber security comes in conjunction with the government's plans to battle crime using technology-based solutions and partnerships"* [14]. With this in mind, the five elements identified above as part of the successful development of a national cyber security strategy [9] are discussed next, in relation to current South African research.

3.1 Political Will

To ensure that the cyber security action plan receives government-wide attention, national leadership is imperative both at an individual and organisational level. Furthermore, national cyber security policies as well as national and international strategies should be in place to fight cyber crime. The draft cyber security policy presented by the DOC aims to ensure that organs of state as well as the private sector can cooperate to ensure the security of South Africa's information networks [14].

As mentioned in Section 2, the South African national strategy for cyber security is under development, albeit not yet implemented or enforceable. The draft policy does address some levels of compatibility with international efforts, as proposed by Ghernouti-Hélie [9]. For example, co-operation between police in the Southern African Development Community region and Interpol is a high priority in 2012 to fight cyber criminal syndicates [7].

3.2 Adapted Organisational Structures

It is recommended that adequate national organisational structures should exist to support the deployment of an effective cyber security solution for individuals, organisations and governmental agencies. These organisational structures should be adapted

from other national models to take elements such as country-specific culture, economic context and ICT infrastructure development into account [9].

In terms of cyber security, a national CSIRT could be the most appropriate organisational structure for linking communication networks and information systems with economic and social development. Earlier South African research has identified nine steps to ensure that the CSIRT meets the needs of such an organisational structure. The first and most crucial of these steps would be clarifying the mandate and policy related issues involved [10]. At the time of writing, a new move towards the development and establishment of one of the South African CSIRTs is underway by the DOC and joint partners. The necessity of national CSIRTs is underscored in the draft South African cyber security policy [8].

3.3 Identifying Accurate Proactive and Reactive Measures

Since everyday activities have an increasing digital component, it is becoming increasingly urgent to augment and automate cyber security in order to maximise outputs and minimise human error. Both South African individuals and groups are largely dependent on data. This dependence relates not only to physical data, but also to the relationship of this data to specific infrastructures. Accordingly, it is important that these actions can be both proactive and reactive in nature.

Ghernouti-Hélie [9] proposed that cyber security actors can be classified into three roles: the protector; the protected; or the criminal. Once the South African cyber security policy is implemented, it is envisioned that the roles would be addressed appropriately, and South African citizens should have a better understanding of where they fit in terms of, for example, who will play the role of the protector, and what is the punishment for the criminals. Existing South African legislation already addresses criminal punishment for cyber security crimes; this includes: the Electronic Communications and Transactions Act No 25 of 2002; the Regulation of Interception of Communications and Provision of Communication-related information Act No 70 of 2002; and the Protection of Personal Information Bill of 2010 [1].

3.4 Reducing Criminal Opportunities

Due to the international scope of the Internet and wide usage of technology, cyber security intersects largely with the application and implementation of international legislation. Regardless, the foundation for an adequate security strategy is twofold: raise the level of risks taken by the criminal, and raise the level of difficulties faced by the criminal. In all instances, legislative and regulatory measures should concomitantly raise the level of risk perceived by a criminal, and decrease the favourable context to perpetrate an illegal action [9]. Reducing opportunities for crime is one of the ultimate benefits of implementing a cyber security policy framework. As such, South Africa is one of the signatories of the Council of Europe's Convention on Cybercrime [5].

3.5 Education and Awareness

Organisational structures should encourage, lead or coordinate continuing education for professionals in the legal, economical and political fields. In addition, the realisation of a global cyber security awareness culture will contribute to achieving part of the goals of a national cyber security strategy [9]. In South Africa, there are several cyber security awareness programmes aimed at educating user groups in different geographical areas of the country [11], made necessary by the increasing rate of bandwidth consumption or utilisation in South Africa. Already in 2007/2008, South Africa's overall online activity was estimated to be 67% of overall online activity in Africa, whilst its population accounted for only 5% of that of entire continent [19]. This emphasises the importance of proper cyber security awareness and formalised training in this domain.

Research done in the South African provinces of Gauteng, Mpumalanga and Limpopo in general indicates good Internet behaviour on the part of South African citizens. Completed questionnaires were retrieved from different geographical areas and were grouped under urban areas, semi-rural areas and rural areas. The levels of cyber security awareness were calculated as 69% for urban areas, 53% for semi-rural areas, and 40% for rural areas. A cumulative extrapolation of total awareness in South Africa based on the overall awareness of the sample group is estimated at 51% [17]. This aspect still requires a lot of attention in South Africa.

The next section introduces the use of an ontology to assist in the development and implementation of a South African cyber security policy.

4 Using an Ontology to Implement Cyber Security

The mapping of South African research and development activities on the five practical elements as proposed for international cyber security policy implementation (refer to Section 3) shows that some progress has been made. The discussions also highlighted the involvement of a number of entities and functions to ensure the successful implementation of a national cyber security policy. However, since the cyber security environment is not clearly bounded and defined, it is very difficult to put forward an easily understandable and implementable cyber security policy. As such, the authors propose to use an ontological model to formally define and describe the roles of players in this environment together with their functions and responsibilities, as well as the roles of the different stakeholders in the cyber security environment. It is important to realise that there are multiple levels of role players in the cyber security environment and that roles and responsibilities often overlap. It is precisely this layer of complexity that necessitates a structured, formal description of the environment before implementation of the policy can succeed.

This ontology will provide a model of the shared environment (i.e. the cyber security domain), a common vocabulary and formal descriptions of the inter-relationships between the relevant entities and functions as identified in Section 3. Ontologies have been used previously to define policy frameworks and instantiate policies [6]. Although the use of an ontology as proposed here is different to that of Cuppens-Boulahia et al., it is

clear that ontologies can be used to assist with the implementation of policy in various ways. Ontologies could therefore be a valuable contribution to the final implementation of a cyber security policy in South Africa.

The methodology of using an ontological model will benefit the communication and sharing of information between role players during the implementation of the policy, the modelling of the implementation phases and functions, and for education and training.

The next sub-section contains an overview of ontologies in general and the subsequent sub-section describes an initial high-level ontology for the cyber security strategic environment.

4.1 What Is an Ontology?

For the purpose of this paper, an ontology is a technology that provides a way to exchange semantic information between people and systems. It consists of an encoded, common domain vocabulary and a description of the meaning of terms in the vocabulary. Grüber [13] defines an ontology as *"formal, explicit specification of a shared conceptualisation"*. A formal ontology specifies a machine-readable domain model depicting entities and their inter-entity relationships. It generally consists of a descriptive part and reasoning technologies. The descriptive part of an ontology captures the domain from the domain experts' point of view, expressing domain information in a way that can be processed by computers and be understood by humans. The use of reasoning technologies enables new information to be derived from the facts contained in an ontology.

The information in an ontology is expressed in an ontology language (logic-based language), and then progressively refined. The construction and maintenance of ontologies greatly depend on the availability of ontology languages equipped with well-defined semantics and powerful reasoning tools. Fortunately, there already exists a class of logics, called description logics (DLs), that provides for both, and are therefore ideal candidates for ontology languages [2]. The Web Ontology Language (OWL) 2.0 was granted the status of a W3C recommendation in 2009, and is the official Semantic Web Ontology language. OWL was designed to provide a common way to process the content of Web information instead of displaying it. It is intended to be interpreted by computer applications and not to be read by people [22]. In this research, OWL was used to interpret the ontological model developed for the cyber security strategic domain.

The use of ontologies is growing rapidly in a variety of application areas, and is the underlying technology driving the Semantic Web initiative [3]. Ontologies vary greatly in their content and intent [4], [25]: upper-level ontologies define general, descriptive terms that are domain independent; core ontologies contain only terms that are domain-neutral, that is, terms that apply to multiple sub-domains; and domain ontologies represent specific terms in a particular domain and are detailed.

4.2 A Domain Ontology for the Cyber Security Environment

There are many benefits to implementing ontologies. As such, the authors used an ontological model to identify and propose a formal, encoded description of the cyber

security strategic environment. This will contribute largely to the development, implementation and roll out of a national cyber security policy in South Africa. Benefits include:

- **To enable the re-use of domain knowledge.** There are many role players in South Africa that have performed research and development work on cyber security. Involving these role players as domain experts in the development of the ontology will maximise the utilisation of any existing domain knowledge.
- **To share a common understanding of domain concepts and information among the members of a community.** Due to the dynamic and volatile nature of the cyber security domain, there are often multiple explanations or ambiguous understandings of domain specific concepts. An ontology will assist in standardising these concepts.
- **To facilitate information integration and interoperability between heterogeneous knowledge sources.** As pointed out in Section 3, entities and functions involved in the cyber security domain range from local to international, humans to organisations, and policies to implementation tools. By using an ontology, it would be possible to ensure integration and interoperability between different components of the larger South African cyber domain.
- **To analyse domain knowledge.** Existing domain knowledge, once identified and captured within an ontological model, can be used to finalise the South African cyber security policy, and implement its components to ensure the better protection of National Security and safekeeping [20].

The main benefit of the high-level ontology envisaged here is that a formal, encoded description of the cyber security strategic environment will be created: that is, all the entities, their attributes and their inter-relationships will be defined and represented. There will be a single shareable model of the environment, agreed-upon by subject experts.

This paper presents the upper-level entities of an initial ontology. Subject matter experts have identified these entities. The proposed cyber security strategy environment ontology is implemented in 'Protégé', a free, open-source platform that provides a suite of tools to construct domain models and knowledge-based applications with ontologies [23]. The main entities in the environment are the *Human Domain*, *Information*, *Infrastructure* and *Tools*. Figure 1 illustrates the main entities and their attributes and relationships.

The Human Domain entity consists of either individuals or groups. A group can be public (e.g. a state department) or private (e.g. a company or a terrorist organisation).

A group has the following attributes: size, goal, role, motivation, and it can be regarded as a target.

A goal is an intended outcome whilst a motivation is related to an individual or a group's needs.

An individual shares all of these attributes, but its size is exactly one.

Humans use tools, measures, guidelines, policies, techniques, applications, etc. and infrastructure to protect or attack information security and to manipulate information.

Infrastructure can consist of physical infrastructure, electronic infrastructure, or software. Infrastructure has a location as attribute.

Information has a type and format as attributes. Information and Infrastructure have a security classification, and Information has Infrastructure (e.g. is stored somewhere).

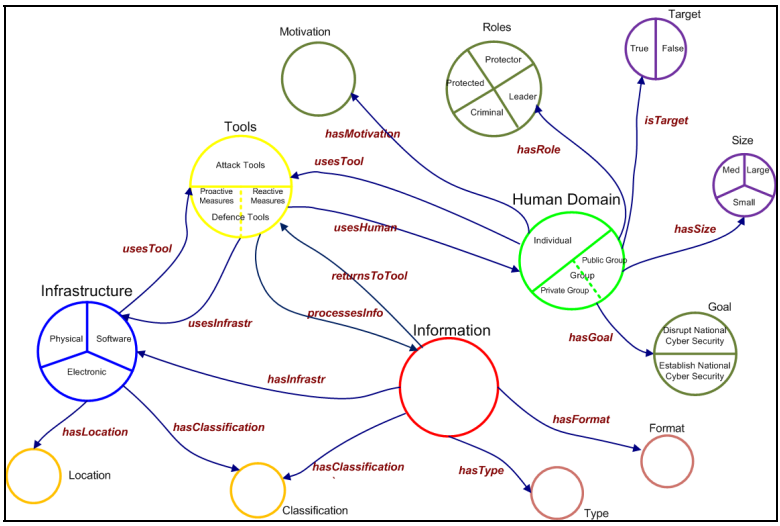

Fig. 1. Illustration of high-level cyber security strategy environment ontology

Cyber security awareness and training are relevant in determining the type of information that must be represented in the ontology, and initial steps have been taken towards the establishment of a Cyber Security Hub in South Africa [19]. This Hub will be responsible for cyber security awareness on a national level. The main role players in terms of cyber security awareness in South Africa are the DOC, the Department of Basic Education, and the South African Police Service (SAPS). A second level of role players includes: Universities and Further Education Training colleges, including the Department of Higher Education and Training; research institutions under the auspices of the DST; non-governmental organisations (NGOs); private organisations; banking sector; mobile sector; MICT SETA (Information Systems, Electronics and Telecommunication Technologies Education and Training Authority); Department of Defence (DOD) and the State Security Agency (SSA); Internet Service Providers; and other government departments.

Most stakeholders have more than one role in the implementation and the application of the policy. For example, DST, the Department of Higher Education and Training and the SSA are jointly responsible for general research on cyber security policy, whilst the SSA takes responsibility for implementing the cyber security policy [15]. Various centres and civil societies in general are responsible for reporting cyber incidents. When a cyber security incident has been reported or a specific instance of the policy has to be implemented, the relevant stakeholders have to be identified and contacted. The initial ontology can be used to support this task.

Fig. 1 only shows the high-level categories of these entities. However, when analysed in more detail, there is a close correlation between the entities identified in Section 3 and the entities in the proposed ontology. For example, the DOC (refer to Section 3.1) can be classified as a public group with the role of leader that uses the cyber security policy as tool (reactive measures) which uses the physical infrastructure of the CSIRT. Citizens (refer to Section 3.3) can be classified as an individual with the role of protected, and an attribute of target. Cyber security awareness programmes (refer to Section 3.5) can be classified as defence tools (proactive measures) that use physical, software and electronic infrastructure in the location of Limpopo.

5 Future Research

The first task in creating the cyber security policy is to set up an implementation framework. The first step must comprise an analysis of the current situation in South Africa. The rationale for this analysis is to break down the implementation into manageable, understandable components, because the role players responsible for the implementation are not necessarily the people who formulated the policy. In addition, the output of the analysis will greatly determine the final organisational structure. It is also necessary to be able to determine the strategies that will achieve the identified objectives of the policy. A final organisational structure needs to be investigated and human, financial, technological and physical resources allocated. A change management plan and commitment plan need to be set up to ensure co-operation between the parties involved. The future research will include:

- Development of the implementation framework;
- Expansion of the analysis of the current structures and role players of cyber security in South Africa. Several other methodologies would be used including Morphological Analysis, a method for systematically structuring and analysing multi-dimensional, non-quantifiable problems [24]. The detailed domain ontologies will be built using all this information;
- Development of organisational structures necessary for implementation of the cyber security policy;
- Extension and implementation of the Cyber Security Awareness Toolkit (CyberSAT);
- Development of change management and commitment plans.

Hence, the use of an ontology is initially envisaged to define the role players and their functions. Later on the authors foresee other uses for an extended ontology. Since the cyber domain environment is vast, a core high-level ontology is proposed to be developed in conjunction with sub-domain ontologies. For example, a sub-domain ontology can be developed for predicting network attacks as a sub-component of the proposed cyber security policy implementation. All the sub-domain ontologies which have been developed can be merged once completed with existing techniques, to provide a combined ontological system that can be further extended.

6 Conclusion

This article describes the implementation of a cyber security policy in South Africa, summarises progress made so far of the research and development performed, and proposes the way forward. The authors discuss the requirements that will enable the implementation of the cyber security policy and reflect on research that is currently being done on the use of an ontology in this regard. The aim of the ontology is initially to provide a formal description of role players and their function in the cyber security environment.

Although several research articles and projects have been undertaken during the last three years, only limited research has been done on the implementation of the cyber security policy in South Africa. The article by Phahlamohlaka [21] discussed the CyberSAT as an implementation strategy. This lack of research could be attributed to the delay in the promulgation of the cyber security policy in South Africa. Cyber security awareness is the only research aspect of the cyber security implementation that has been covered in some detail since 2009, with several players starting to implement some awareness training in South Africa.

References

1. Acts: Acts Online (2012), http://www.acts.co.za/ (accessed March 28, 2012)
2. Baader, F., Calvenese, D., McGuinness, D., Nardi, D., Patel-Schneider, P.: The Description Logic Handbook: Theory, Implementation, and Applications. Cambridge University Press, Cambridge (2003)
3. Berners-Lee, T., Hendler, J., Lassila, O.: The Semantic Web. Scientific American 284(5), 33–43 (2001)
4. Boury-Brisset, A.: Ontological Approach to Military Knowledge Modeling and Management. In: Symposium on Military Data and Information Fusion, Czech Republic, Prague (2003)
5. Council of Europe: Convention on Cybercrime. CETS No.: 185 (2010), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG (accessed March 28, 2012)
6. Cuppens-Boulahia, N., Cuppens, F., de Vergara, L., Vázquez, E., Guerra, J., Debar, H.: An Ontology-based Approach to React to Network Attacks. International Journal of Information and Computer Security 3(4), 280–305 (2009)
7. Davis, G.: State Security in Charge of Cybercrime Plans (2012), http://www.iol.co.za/dailynews/news/state-security-in-charge-of-cybercrime-plans-1.1238243 (accessed February 21, 2012)
8. Department of Communications: National Cybersecurity Policy Framework for South Africa – Draft. Unpublished document (2011)
9. Ghernouti-Hélie, S.: A National Strategy for an Effective Cybersecurity Approach and Culture. In: ARES 2010 International Conference on Availability, Reliability and Security, Krakow, pp. 370–373 (2010)
10. Grobler, M., Bryk, H.: Common Challenges Faced During the Establishment of a CSIRT. Presented at the ISSA Conference 2010, Sandton, South Africa (2010)

11. Grobler, M., Flowerday, S., Von Solms, R., Venter, H.: Cyber Awareness Initiatives in South Africa: A National Perspective. In: Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW 2011), pp. 32–41 (2011)
12. Grobler, M., Dlamini, Z.: Global Cyber Trends a South African Reality. In: Proceedings of IST-Africa Conference (IST-Africa 2012) (2012)
13. Grüber, T.: A translation approach to portable ontology specifications. Knowledge Acquisition 5, 191–220 (1993)
14. Guy: Cyber Security Policy Will Go Before Cabinet For Approval This Year (2011), http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=13783:cyber-security-policy-will-go-before-cabinet-for-approval-this-year&catid=48:Information%20%20Communication%20Technologies&Itemid=109 (accessed February 24, 2012)
15. ICT Procurement: Cyber Security Mandate Transferred (2012), http://ictprocurement.com/security/cyber-security-mandate-transferred.html (Accessed May 3, 2012)
16. Internetworldstats: Internet Usage Statistics for Africa (2012), http://www.internetworldstats.com/stats1.htm (accessed February 27, 2012)
17. Jansen van Vuuren, J.C., Grobler, M.M., Zaaiman, J.: The Influence of Cyber Security Levels of South African Citizens on National Security. In: Proceedings of ICIW 2012, Seattle, USA, pp. 138–147 (2012)
18. Kramer, F.D.: Cyberpower and National Security: Policy Recommendations for a Strategic Framework. In: Kramer, F.D., Star, S.H., Wentz, L.K. (eds.) Cyberpower and National Security, pp. 3–23. Centre for Technical and National Security Policy, Washington (2009)
19. Moyo, A. , Kayle, A.: DOC Calls for Collaboration, Security Innovation (2012), http://www.itweb.co.za/index.php?option=Com_content&view=article&id=54874 (accessed August 8, 2012)
20. Noy, N.F., McGuiness, D.L.: Ontology Development 101: A Guide to Creating Your First Ontology. Technical Report KSL-01-05. Stanford Knowledge Systems Laboratory (2001)
21. Phahlamohlaka, L.J., Jansen van Vuuren, J.C., Radebe, J.: Cyber Security Awareness Toolkit for National Security: an Approach to South Africa's Cyber Security Policy Implementation. In: Proceedings of the First IFIP TC9/ TC11 Southern African Cyber Security Awareness Workshop 2011 (SACSAW 2011), Gaborone, Botswana, pp. 1–14 (2011)
22. OWL 2 Web Ontology Language (2012), http://www.w3.org/TR/owl-overview (accessed March 27, 2012)
23. Protégé ontology editor (2012), http://protege.stanford.edu/ (accessed February 7, 2012)
24. Ritchey, T.: Wicked Problems. Structuring Social Messes with Morphological Analysis. Adapted from a lecture given at the Royal Institute of Technology in Stockholm (2004), http://www.swemorph.com/downloads.html (2005)
25. Smith, B., Miettinen, K., Mandrivk, W.: The Ontology of Command and Control. In: Proceedings of the 14th International Command and Control Research and Technology Symposium, Buffalo, National Centre for Ontological Research, New York (2009)